~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

4th Issue, 1987

HOW TO WIN WITHOUT PLAYING THE GAME . . . . . [redacted] .1
LETTERS 5, 10
PROJECT TIPONI. . . . . [redacted] .6
THE EFFECTS OF DETONATIONS ON METEOR SCATTER. . N. C. Gerson. . . .9
BULLETIN BOARD. 10
ALAS, WADE GILES, I KNEW YOU WELL . . . . . Leigh Sawyer. . . 11
HOPEFULLY, FOR ALL OF WE. . . . . [redacted] 12
THE MATTER OF STYLE . . . . . [redacted] . . . 14
HOW TO MEASURE CLARITY IN WRITING . . . . . [redacted] . 15
TWO TIPS ON WRITING . . . . . [redacted] . . . 16
POINTERS ON GRAMMAR . . . . . Ralph Jollensten. 17
THE HERO OF THE SENTENCE. 18
GIMME REWRITE!. . . . . Va. 19
BOOK REVIEW: MACHINE TRANSLATION. . . . . [redacted] . 20
FROM THE PAST 21
BUSMAN'S HOLIDAY: A BRITISH CIPHER OF 1783. 22

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIV, No. 4 ..... 4th Issue 1987

PUBLISHER .....

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization,and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

DESERT ISLAND BOXES

The scenario below was inspired by the program on public radio, "Desert Island Disks" where guests select five recordings and one other item to while away the hours when they are castaways on a desert island. The guests also discuss their choices and philosophize on their careers and on life in general.

We thought it might be fun for CRYPTOLOG readers to think out a version of this fantasy.

⊕ ⊕ ⊕ ⊕ ⊕

You're shipwrecked on a desert island on your way to a field site. You've got everything with you to carry out your mission, packed in boxes that are 12x12x15. And thanks to miniaturization, a pc and printer fit in one box. Fortunately, in the desert island there is food, shelter, clothing, and standard supplies aplenty, as well as electricity. Also, your team can communicate with the main frame at HQS via a pc for a total of an hour a day. But you will have to take along the references and handy-dandys, in the form of paper, floppy disks or other media, that you will need to accomplish your mission.

Each member of your team is allowed to take along six boxes, five with materials for the mission that are selected and packed by that member, and one for personal use, relaxation or otherwise. There's a catch, however: the team may be evacuated to another island, in which case the team leader may be ordered by HQS to jettison one mission box per person.

What would you take with you? How would you pack your boxes? All your dictionaries, say, in one box, or lesser ones in the jettison-able box? And why? What would you put in your personal box, and why?

It will be most interesting to read your responses.

How to Win Without Playing the Game

P.L. 86-36

On International Protocol Standards and Security Features for DoD

[redacted] R536

(U) As the International Standards Organization (ISO), and by extension, the American National Standards Institute (ANSI), continue to specify inter-computer protocol standards for open systems, more pressure is being put on the DoD to adopt these standards. Upon completion of the study of the National Academy of Engineering, comparing DoD's Transmission Control Protocol (TCP) with ISO's Transport Protocol Class 4 (TP4) for use in DoD, the Assistant Secretary of Defense for Communications, Command, Control, and Intelligence stated that DoD will transition to the international standards once they have been shown to be as reliable and resilient as current DoD protocol standards. NATO has already endorsed for NATO systems the use of protocols developed from these standards.

(U) A benefit advanced for adopting such standards is procurement off-the-shelf as part of a vendor's standard product line. But some major pitfalls lurk in this strategy (or desire) which we will address later.

[redacted]

PITFALLS OF IMPLEMENTING STANDARDS

(U) Significant attention is being given to the ISO reference model and the standard protocol specifications that derive from it. Manufacturers are selling their future products with the words "we are compatible with the ISO standards" or "our system is compatible with

EO 1.4.(c)
P.L. 86-36

the ISO reference model." Purchasers seem to be of the belief that products purchased with the ISO caveat will allow those equipments to intercommunicate automatically with products with the same caveat from other vendors.

(U) However, few people at high levels seem to be paying attention to what really matters, which is the implemention, not specification, of the standards. The American and European continents have different approaches to implementation. Additionally, implementations are jealously guarded, usually with comments like "don't worry how I implement them internally, as long as I provide the standard interface, you shouldn't care."

(U) I believe that the European market is so small that any single vendor cannot capture a large enough market share to remain profitable. It is therefore, to their advantage to be able to interoperate with each other's equipments. In the US, however, the market is sufficiently large that a number of vendors can each capture a profitable market share, thus affording less incentive to interoperate with other vendors' equipments. These vendors are "adopting" the ISO approach, but they are doing this either in conjunction with their own proprietary approach, or by adding proprietary functionality which can result in non-interoperability. Moreover, each vendor attempts to add its own little enhancements which try to lock in their customers to *its* equipments, and prefers to implement its own proprietary protocols and network architecture. By contrast, European vendors predominately are planning to adopt ISO and to discontinue their own proprietary approaches.

(U) Some US vendors are adopting the International Standards as a second capability to try to meet the requirements of some of their users who are adamant about the use of commercial standards. But what isn't said is how they will go about providing them. In addition to incompatible enhancements to the international standards, some vendors have privately indicated that they may provide "invisible" translating gateways between the international standards and their proprietary protocols. Effectively, they are providing an ISO interface into their proprietary network. The interconnection of their machines runs only their proprietary protocols. For those US vendors who take one of these approaches, statements of compatibility with ISO protocols are at best a smoke screen to obscure what they are really doing, and at worse, misrepresentation of their products.

(U) The original intent of the DoD Protocol Standardization effort was to preclude the need to translate protocols by requiring all to implement a standard protocol suite. The ISO standards are based on the same premise. But as things stand now, let the buyer beware. Each individual vendor's approach needs to be carefully examined.

IMPLEMENTATION OF PROTOCOLS WITH SECURITY MECHANISMS

(U) The pit becomes larger when security features are included in protocol implementations. There are three elements to the inclusion of security features in protocols: the definition of the security mechanisms; the implementation of those mechanisms in a trusted way; and the assurance that the implementation is in fact correct and safe. Security mechanisms are normally included as part of the protocol specification. However, protocol specifications do not address either trusted implementations or assurance factors. The ISO Security Addendum deals primarily with security mechanisms and their placement in an overall protocol architecture, the ISO Reference Model. It mentions that trusted functionality is expected whenever security features/mechanisms are implemented, but it doesn't say much more than that. And for its purpose, it probably shouldn't. No documents deal with the assurance issue for security mechanisms in protocols, though one that does address assurance is the "Orange Book."

(U) It is clear, I hope, that trusted implementation and assurance issues are (in part) implementation issues. Security mechanisms need to be carefully implemented, understood, and evaluated. Yet it is not clear that vendors fully appreciate the impact of these statements on their freedom over their implementation. One can't allow a vendor attitude of "leave the implementation to me." It is also not clear how much the vendors intend to do about satisfying the need for trusted implementations and satisfaction of assurance requirements.

(U) Will off-the-shelf vendor products be good enough? It is not inconceivable that the DoD may have to modify and/or adapt off-the-shelf

products to meet assurance and security evaluation requirements, as well as to adapt them to a trusted implementation. This is independent of the presence or absence of adequate security mechanisms in the protocol.

AUGMENTING THE INTERNATIONAL STANDARDS

(S) [redacted] In general, it is not clear that this approach can be effectively utilized. It is applicable for simple functionality substitutions, such as replacing one checksum with another. But it breaks down quickly with more complex functionality, especially with the more complex counters against denial of service and integrity attacks.

(U) If one changes the functionality of a protocol, for example, a reassembly scheme to protect against playback attacks, one actually has defined a new protocol. It really doesn't matter how you refer to it, the odds are it won't interoperate with its parent. An excellent example of this name game taken to an extreme is the International Standard Transport Protocol (TP) and its versions TP0 through TP4. In actuality, they are five different protocols that do not interoperate with each other. Yet because purists in ISO will allow only one protocol per layer, they defined these different protocols as versions of the same protocol. Some even claim that the National Bureau of Standard version of TP4 differs from ISO's TP4. Its not clear whether implementations of the two will in fact interoperate.

(U) However, there is an excellent concept in the previous suggestion. That is the modification and/or augmentation of off-the-shelf protocols. We can combine that concept with a few others to define one possible approach of utilizing international standard protocols to the maximum extent possible, without active involvement in the standards arena.

(U) We begin by first recognizing that any protocol functionality of a non-sensitive and unclassified nature can be presented and argued by the National Bureau of Standards. They are the Government's agent in the commercial standards arena. This method of operation can continue.

(U) We next look at NATO's method of operation. They first try to get ISO to adopt their military requirements in the commercial standards. But they recognize that not all military requirements are needed by the commercial world, and that they won't all be accepted. They have Standard Nation Agreements (STANAGs) which are basically NATO augmentations of commercial standards for NATO's use.

(U) Now the questions become: can a similar bureaucratic approach be used by the DoD, and can implementations be structured in such a way as to make the approach acceptable to all parties? We propose that DoD develop the equivalent of NATO STANAGs for DoD purposes, as part of the DoD Protocol Standards Program. Where the augmentations or changes deal with sensitive security issues, there is nothing to prevent the DoD augmentation from being classified. It appears that some bureaucratic mechanisms are already in place, with a DoD Protocol Standards Steering Group report identifying the "development of Mil-Spec supplements for the commercial ISO protocol definitions."

DEVELOPING THE IMPLEMENTATION

(U) The more difficult question is, can off-the-shelf implementations be easily modified? And how can the new version be structured so that the old version could still be utilized if necessary?

(U) We will start by examining what the conditions are if the desire of using off-the-shelf products containing security mechanisms were achieved. It would have to be a trusted implementation. It would have to be evaluated, and therefore understood by independent parties, and it would have to meet some assurance level of correct and safe operation. All of these criteria argue that the implementation would have to be well structured, most likely in a modular way.

(U) Our approach, where a DoD product is derived from an augmented off-the-shelf product, would still require it be modular. But it would not necessarily require that the off-the-shelf implementation be a trusted one. Additional security functionality modules could

be added, and calls at the appropriate places in the off-the-shelf version could be inserted. Where functionality has been changed, the module calls in the off-the-shelf version would be changed to call the new modules.

(U) Alternatively, a conditional test of whether or not one was operating in secure mode could be added with a call to the new module. This would allow continued operation of the original product as well. Using the terms of protocol implementers, the security functionality would be viewed as "optional functionality," which is not invoked for non-secure operation but which would always be invoked for secure operation. This approach also allows for a more complex implementation whereby the security system may back off from some of the features provided if environmental conditions warrant it and if policy allows it. (An example of a security back-off is BLACKER's Emergency Mode.) This is not to suggest that back-off be a user-selectable option.

(U) The only modules that would need to be protected and evaluated would be the new ones. Thus, a trusted computing base could be designed around only the new modules, leaving the rest of the protocol to run as untrusted code. The trusted computing base would also have to ensure that the secure functionality is invoked for secure operation.

(U) One must recognize the performance risk with modularly implemented protocols. The overhead associated with module calls and returns can be significant, and may have a negative impact on the ability of the implementation to meet high speed performance requirements. Careful design in this area is required. A proof of concept demonstration in this area would be reassuring. (C324 is addressing the issue of protocol implementations in ADA. ADA alone forces a high degree of modularity in an implementation.)

(U) Of course one does not change the functionality of a protocol without changing the headers. If one adds functionality to the basic protocol, then the header must be extensible, with option fields being used for the new functionality. If a functionality change requires a header field change, two approaches could be used. One is to use the option field approach, where the presence of the option field overrides the correspondent field in the basic header. Or, one could define a different header format from the basic one, and distinguish between them through the use of a protocol version number in the header.

CONCLUDING REMARKS

~~(C)~~We believe this to be one approach which would satisfy the contradictory desires to use off-the-shelf commercial protocols as much as possible and still prevent transfer of security technology potentially inimical to DDO's mission. This approach does not require active participation in the commercial standards world. We take what they produce and modify it appropriately, through the DoD Protocol Standards Program for the specifications, and through vendors or cleared contractors for the implementations. Contractors and vendors could be restricted as to whom they provide the "DoD secure" implementations.

(U) What is required of the international standards is only an extensible header and a protocol version number in the header. What is required of the implementation of the standard would be modularity.

(U) It has also been argued that the US commercial world is also in need of security protection. This is a major argument for NSA's active involvement in the international standards process. By using the above approach, commercial vendors could be provided the security modules (DoD specifications or implementations) under a license arrangement, which could restrict dissemination of the "DoD-secured" product in any manner DoD required. It could be restricted to continental US use, to US-owned companies, etc. This approach is analogous to the COMSEC Commercial Endorsement Program licensing arrangement for encryption implementations.

(U) The serious technical implementation challenges of this approach are a modular implementation (which would be required anyway for a trusted implementation) with adequate performance, the manner with which the "security modules" are integrated into the commercial product, and the ability to run an off-the-shelf implementation as untrusted code on a trusted computing base. One conjectured approach for doing this, utilizing ADA, has already been raised.

(U) This approach does not satisfy the desire by some defense personnel to actively participate in the international and national commercial standards arenas for security enhancements. Some seem to have confused the means with the ends.

ACKNOWLEDGMENTS

~~(FOUO)~~ I wish to thank [redacted] C322, and [redacted] R536, for their helpful comments on an earlier draft.

SOURCES AND REFERENCES

(1) ISO Draft Standard 7498, Open Systems Interconnection (OSI) Protocol Reference Model

(2) ISO 7498 Part 2 Draft Proposal, Security Addendum to the OSI Reference Model dated Nov 85

(3) Transport Protocol for Department of Defense Data Networks; National Research Council Committee on Computer-Computer Communication Protocols

[redacted]

(5) DDO contribution to (9), 3-page paper undated and untitled.

(6) M/R serial C3-160-82 dated 2 Nov 82; subj: National and International Standards, DoD Use Thereof; Network Security Issues, and Classification

(7) Q41 Memorandum dated 3 Jul 86; serial Q4-637-86; subj: Final review of Network Security Classification Guidelines

(8) M/R serial C32-003-84 dated 18 Jan 84; subj: Status for NSA Response to USD R&E (CCCI) on Use of Commercial Standard Protocols in DoD

(9) DIRNSA letter N1743; dated 18 Oct 84; subj: Data Communications Protocols

(10) Department of Defense Trusted Computer System Evaluation Criteria, National Computer Security Center

(11) Q41 M/R (no serial) dated 6 Aug 86; subj: OSD Initiative re Participation in Standards-making Bodies

(12) C Memorandum C-301-84 dated 31 Aug 84; subj: Data Communication Protocol. (The ADCS contribution to (9))

(13) C Memorandum C-367-82 dated 9 Nov 82; subj: Classification Guide for Network Security

(14) Private conversation with vendor personnel at the National Academy of Engineering Transport Protocol Study which resulted in (3)

(15) DCA/DCEC/R130 letter dated 21 Aug 86; subj: Record of the 27th Meeting of the Protocol Standards Steering Group (PSSG), 24 June 1986

P.L. 86-36

To the Editor:

(U) As I walked into the office early this morning and saw our latest intern hard at work, these thought flooded my mind. With only one or two exceptions, the 15 or so interns the division has enjoyed in the last 3 years have been super performers. We've given them responsible jobs and challenged them to excel. They have taken up the challenge and produced results far above our high expectations.

(U) I've heard expressions of concern for this Agency's eroding experience base. I've also observed that long experience, per se, isn't always relevant, and is sometimes an impediment, to solving current problems. If the interns we've had are representative of the intern popiulation as a whole, and I have no reason to doubt that they are, then the Agency's future is in quite capable hands. These young folks may not always do things the way we old-timers would, and that may be good.

[redacted] *P36*

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

Project TIPONI

The Translator's Workstation of the Future

[redacted] *P16*

P.L. 86-36

[redacted]

Description of the Task

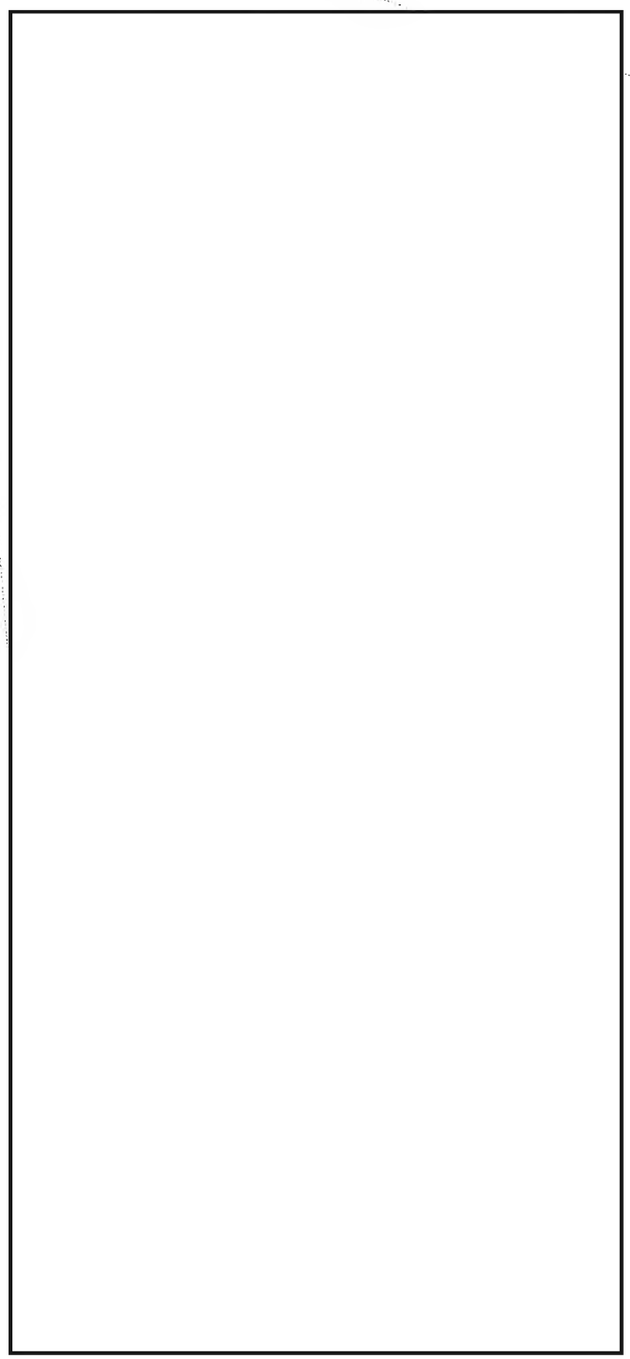
[redacted]

(U) We also require the capability to optically scan hardcopy data, in any native script, for input to the workstation in the native script.

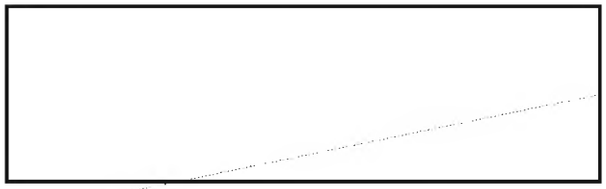
[redacted]

EO 1.4.(c)
P.L. 86-36

Selecting Reportable Messages



The Translation Process



(U) As he works, the linguist may wish to jot down notes on either the message text or the translation. The notes should be clearly distinguishable from the text itself and should be deleted easily when the translation or report is complete, if desired. For example, the linguist may wish to send notes along with the document to another linguist noting an area with which he had difficulty and where he requires assistance.

~~(FOUO)~~ During the process of preparing a message for publication the linguist needs to consult on-line working aids such as gazeteers, dictionaries, special purpose glossaries, databases, etc. to obtain further information about a name, location, or another message referenced in the message in question. These on-line tools should be easy to reference and easy to display in a small window where it does not obscure the rest of the text. During the process of preparing the report, the linguist may add footnotes to the end-product. The footnotes should be automatically placed at the end of the document and in the appropriate format. In checking his work, the linguist may wish to examine the footnote at the same time that he is looking at the text which is footnoted.

~~(FOUO)~~ After the translator has completed a report or translation, he prepares a cover sheet for the end-product and sends both to a senior linguist or checker who verifies the accuracy of the coversheet and of the end-product. The linguist may wish to display the source text, translation, and cover sheet on the screen at the same time.

(U) The checker may consult on-line working aids such as dictionaries and glossaries, and

P.L. 86-36

should be able to look at a footnote as he is reading the footnoted text. The checker may wish to jot down notes on the document in order to direct the linguist's attention to errors to be corrected, or to train a junior linguist. These notes should be clearly distinguishable from the text and easily deletable. If the text is returned to the linguist for corrections, it is then returned to the checker who will look at the notes and corrections to verify that the document is now correct. When the document is approved, the checker sends it along to another workstation for publication, or a camera-ready final copy is printed.

Summary of Desirable Features of a Translator's Workstation

Screen Size

(U)The display for a translator's workstation should be large enough to allow a linguist to look at large portions of both the original text and the translation so that he can see enough information to understand the text. There should also be room for small windows to display working aids such as dictionaries. This requirement probably calls a 19-inch screen with bit-mapped graphics display. The 11-inch or even larger raster displays are not large enough or flexible enough to offer a linguist an alternative to paper and pencil.

Fonts

(U) In some cases for display of the text, and in many cases for display of softcopy working aids, linguists require foreign language fonts in approximately 30 to 40 foreign writing systems. The foreign fonts must include punctuation and special symbols necessary to represent the foreign language accurately, and the display screen must have sufficient resolution to represent the native scripts clearly and accurately. The fonts required include difficult ones such as Japanese, Chinese, and Korean, as well as the easier European languages. A variety of font sizes and faces should be available to highlight portions of text.

Word-Processing

(U)The foreign language displayed must be in a form, i.e. character strings rather than graphics or pictures of text, that can be edited, sorted, indexed, parsed, etc. The user must be able to specify how the text is to be sorted or indexed, including the direction (forward or reverse), nulls, etc.

On-line Working Aids

~~(FOUO)~~ Linguists require softcopy working aids such as dictionaries, gazeteers, [redacted]lists, etc. which can be referenced from the workstation. The dictionaries should include both personal dictionaries and master dictionaries available to all linguists. New additions to the dictionary would be added to the personal dictionary, and be stored in a file for review by a senior linguist before being added to the master dictionary. The dictionaries must be capable of including grammatical information, usage examples, English translation, and descriptive narrative in English, the foreign language, or both. The grammatical information should be stored in concise linguistic format to save space, but be expandable by a user interface so that the information could be used by language specialists who are not familiar with the formal notation system.

Translator's Editing Features

(U) The checker requires capability to show on the screen the suggested changes to the product in order to assist in training junior linguists. This would include such things as pointing out omissions in the text, errors in the text, suggesting deletions in the text, indicating with highlighting, pointers, lines, or color, dependency relationships in the text which the translator has failed to understand. □

The author solicits comments from linguists and reporters who might be concerned with any aspect of the process described.

The Effect of Detonations on Meteor Scatter

N C Gerson, W3

~~This article is classified CONFIDENTIAL in its entirety~~

Meteors create discernible ionization trails at altitudes between 60 and 140 km above the earth. On the average, the trails last for seconds or less. The electron densities in the trail usually range from 10^6 to 10^8 per cm^3. These figures represent nominal means of distributions; extremes are larger in all cases.

Meteor scatter systems offer low data rate circuits at high reliability, low power and some privacy.

If sufficient ionization arising from any other physical mechanism is produced in the altitude range near 100 km, the meteor system operates continuously as a normal system. This may occur under either of two conditions:

- natural, when sporadic E is present, or during periods of high sunspot activity;
- man made, during artificial modification of the E layer, or during high altitude nuclear detonations.

Effects of the latter are discussed below.

High Altitude Detonations

A high altitude detonation may be defined as one that occurs above 40 km, where atmospheric number densities approach those in vacuum – or discharge – tubes. The detonation releases huge amounts of energy, both radiant (to gamma rays) and corpuscular (ionized metallic and atmospheric species lumped together under the term debris). The injection of this energy at this altitude profoundly alters the normal ionosphere.

It should be recalled that energy of this magnitude injected into the ionosphere produces complex hydrodynamical and magneto-hydrodynamical disruptions, and changes the ambient chemistry and ionization reactions. After a single detonation, the entire affected area remains violently disturbed for 30 to 60 minutes.

EO 1.4.(c)
P.L. 86-36

Finally, it must be remembered that the ionosphere is self-healing. After a period, whose duration depends on the total energy and on the altitude of the detonation, the ionosphere slowly returns to normal under the action of sunlight. □

MOVING?
Mail a change of address to:
HQS, P1, Editor, CRYPTOLOG
Include your Name, Old and New Organization, and Old and New Building

BULLETIN BOARD

ANALYTIC SOFTWARE FOR PCs

~~(FOUO)~~ A new work center in G33 is being created specifically to provide support on the pcs for the exploitation of manual systems in G Group. This center will offer personal help as well as generalized and customized programs. All it takes is a phone call. In addition, it will maintain a library of cryptanalytic programs for the ASTW. In the future it will call for programs written in G and elsewhere that could be used by a wider audience.

~~(FOUO)~~ The new center will be headed by [redacted] 963-3669. Other pc needs will continue to be provided by G331, whose chief is [redacted] Her phone number is also 963-3669.

P.L. 86-36

GERMAN TV HOUR

(U) If there is sufficient interest, we will resume showing TV news and documentaries in German from the FRG, Austria, and the GDR. In the past they were shown once a week at lunchtime on a walk-in basis. Let us know how often you'd be likely to attend (once a week, once a month, etc.) Please respond to [redacted] P16, HQS 8A187, 963-1103.

P.L. 86-36

To the Editor

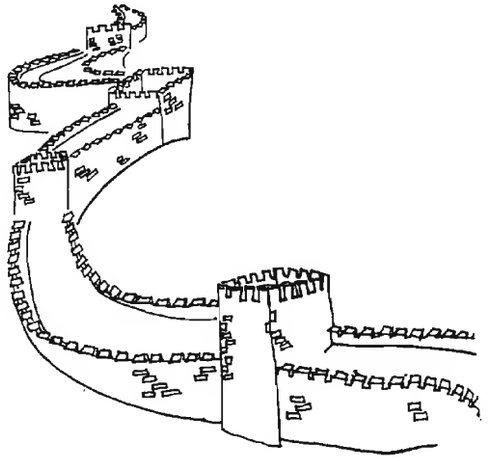
I enjoyed Dave Chizum's article on Ethiopia [CRYPTOLOG, 1st Issue 1987] so very much. It's a thrilling and exciting story - and a first-rate piece of writing. It's too bad it's classified and can't be published outside.

[redacted] *SC*

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

ALAS, WADE GILES, I KNEW YOU WELL



E. Leigh Sawyer, Ret.

In the December 1972 issue of the now defunct publication *DRAGON SEEDS*, there appeared an article of mine on the Wade Giles system. This system for the romanizing of Chinese, once used by NSA and throughout the intelligence community, was cast aside on 1 January 1979 in favor of the PINYIN system. For historical purposes, it might be well to reprint the Wade Giles item if only for auld lang syne. By the same token, a PINYIN item would also seem appropriate so as to permit a better understanding of how the system works.

THE WADE-GILES SYSTEM

For the p'erson who has had little exp'erience with the Ch'inese lankuache, the p'ronouncing of p'lace names, p'eop'le's names, art'ifak't's, and even the inkretinent's of Monkolian parpek'ue is often k'onfusing. An unterst'anting of at least Wate Chile's ap'ost'rophic usache aft'er cert'ain k'onsonant's chust might enable one t'o atchust himself t'o this esot'eric linkuist'ic area. A little pak'ground on Wate Chiles might pe in orter. Wate Chiles was porn in Ch'ik'ako, and lat'er moved to Cheorchia. At that t'ime, his mother atvised him, "You ought t'o invent something. Why ton't you ko t'o Ch'ina, Wate, and invent the Wate Chiles syst'em?" He said, "Poy oh poy, mom, puy me a t'ik'et and I will t'ake the first poat leaving p'ort." So he t'ook off for K'athay. His letters t'o his mother reflek't the choy he felt in t'raveling from p'lace to p'lace. He mate reference t'o the many intichenous t'ype nat'ives he had pump'ed int'o, and the cheokraphik'al ottit'ies he had seen. In any k'ase, as may be kauched py it's witesp'read usache t'otay, Wate invent'ed his syst'em, and it is seen on map's and all k'inds of swell st'ull all over the p'lace.

On the pasis of the k'arefully kathered tat'a p'rovided apove, one k'an easily tecite how t'o p'ronounce that p'art of a Ch'inese p'lace name that has an ap'ost'rophe in it, and one which toesn't - also p'rop'er names (poys or kirls) and telek't'aple Ch'inese tishes such as K'ant'onese st'yle pean k'urd.

THE PINYIN SYSTEM

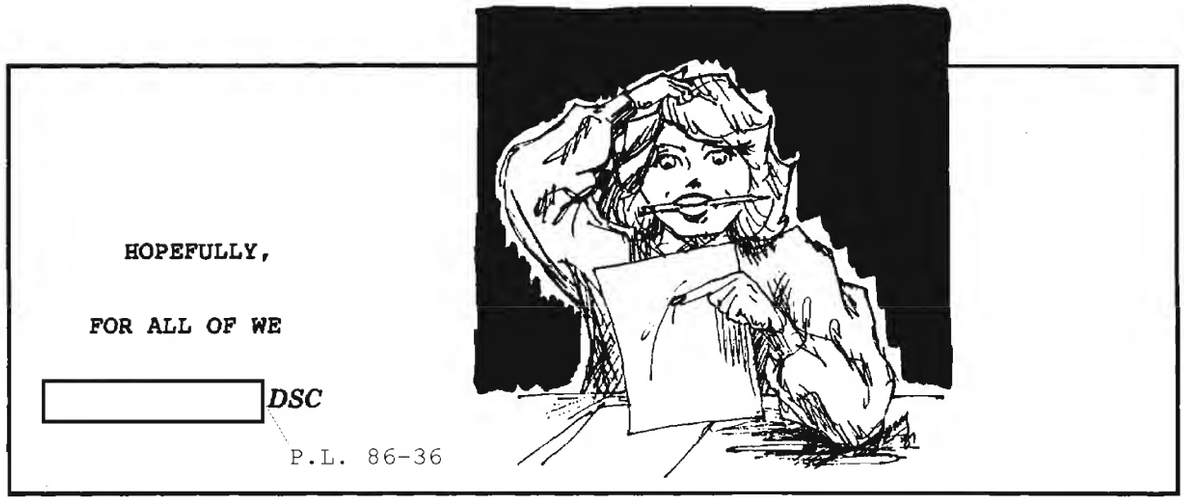
Wonce upon a taim, there were tu little Chinese boyis named Pin and Yin. Won night, Pin was studying Chinese karakters when he suddenly threw down his book and said to Yin, "Anyone hu studies this zhunk has to be a zherk. What du you say tu our killaborating on a niu system. We'll kall it the "Pin-Yin' system'." Yin said, "Don't hand me that zhaive. That would bi qiting on the system. It's ok to qit at ma zhoung or at kads, but not in skul. Bisides, if we went ahead with a niu system, we should kall it 'Yin-Pin'."

Well, they qiued this over for a bit and finally agreed on "Pin-Yin." The mein-reason being Pin kud easily punch out Yin bikause he was a lot bigger. The top of Yin's head only kame to Pin's qin.

"Anyhow," Pin said to Yin, "If we are tu get on with this, we'd be waise to du it on a full stomak." So, after a big meal of fish head and ternip chaoder, and also raiding the kukie zha, they set to work.

Working dei and night, they zhenerated the system in short order. When they were finished, they went tu the zhuish deli around the kourner for beigles and a kup of zho. "Ji whiz," said Pin tu Yin, "won't Wade Zhailes be mad when he learns of our system? He may try tu send us to zheil, may be even to Xing Xing."

Well, Pin and Yin did not go tu zheil. The moral of this story being, there's more than wun wei to skin a kat, so qin up, Wade Zhailes dai hards, and bi of good qir. □



In my article, "How To Write A Memo" published in CRYPTOLOG, 1st Issue, 1987, I promised some pointers on grammar. Here they are. Grammar is such a problem these days that I have about given up on it, and I debated with myself about tackling it in this article. But I'll give it a try. I must say something about a few errors, at least the ones that bother me the most and interfere seriously with my ability to understand memos and almost everything else I read as well.

¶

One of my pet peeves is the misuse of **hopefully**. If you want to make me cringe, just use that word. Until recently, **hopefully** was just another common adverb meaning "with hope."

He eyed the candy jar hopefully (with hope).

He approached the task hopefully (with hope).

But at present it's commonly misused. One doesn't really mean this:

Hopefully (with hope???) he'll make the next touchdown.

But this:

I hope he'll make the next touchdown.

I urge you not to use **hopefully** at all if you can't use it correctly. If you mean "I hope that" then say it, and do not misuse the adverb **hopefully** (meaning "with hope") instead. Don't be a lamb following all the others into this error!

And while I'm talking about "ly" words, here is another: **most importantly**. That also sets my teeth on edge. Only rarely is it the correct phrase. Most of the time the ly is redundant and ungrammatical. Say "most important" since that is what you mean.

¶

Apostrophes are everywhere these days and mostly where they shouldn't be. Take its and it's, for example. It's means "it is." The apostrophe represents a contraction:

It's too bad you can't come.

(It is too bad you cannot come.)

Its is a possessive adjective and never has an apostrophe:

Its place was already taken.

Other words of the same type are **his, her, our, your, their** and **whose.**

Hers was already taken.

Hers is a pronoun denoting relation or possession, as are **his, ours, yours, theirs,** and **whose.** In this case I can understand why it's confusing. Ordinarily you make something possessive by adding an apostrophe and an **s.**

In other instances, however, you do indicate the possessive by adding an apostrophe and an **s.** Different books provide differing guidance on use of apostrophes for forming the possessive. But the following simple rules are quite acceptable and will take care of most needs.

1. If a word does not end in **s,** add an apostrophe and an **s:** girl's, man's, men's, people's.

2. If a singular word ends in **s,** add an apostrophe and an **s:** Lois's, James's, Perkins's.

3. In plural words ending in s, add an apostrophe only: girls', boys', wives'.

Which brings me to two common misusages of apostrophes. The first example naturally upsets me because it involves my own name, which happens to end in an s. I can't tell you how many times I have received memos with it written this way: [redacted] office." Of course, this changes my name to [redacted] which it is not. A simple "Mrs. [redacted] office" will do nicely, thank you. Or else you can leave off the final s and write [redacted] office" instead.

The second example is even wilder. It shows that the writer simply does not know the difference between singular and plural. Some hilarious things can result, of course. The best one I've seen, and I see it every night on the way home, is a sign in front of a housing subdivision which reads: "Settler's Landing." Every time I pass it I think about how lonely that single pilgrim must have been!

¶

Will we ever get **affect** and **effect** sorted out? It's really easy, but lately one so rarely sees or hears these words used correctly.

Affect means "to influence." It is a verb only. *Your answer **affected** (influenced) my thinking.*

Effect means "to bring about or to achieve" as a verb. *This proposal could effect (bring about) some profound changes.* **Effect** means "the result" as a noun. *The **effects** (results) of all this are obvious.*

¶

And what about **lie** and **lay**? **Lie** means to recline; it never has an object. **Lay** means to put, place or set down; it always has an object when referring to present time.

A man can **lie** down to rest, but he must **lay** down his head to do so.

When the action has already taken place, note the past tense of **lie** (whose principal parts are lie, lay, lain):

*A man **lay** down to rest ... and **laid** down his head to do so.*

¶

And then there are quotation marks! Judging by the epidemic use of quotation marks these days, a lot of people are saying a lot of quotable things! But that's not the case, of course. What is happening is that quotation marks are misused for emphasis. One of my favorites is a sign I saw recently which said in large letters:

"NO TRESPASSING"

Now what original wit said that?

In general, if you are not quoting someone directly or giving the title of something, don't use quotation marks.

¶

To conclude, I'll say something about the current misuse of **I** and **me**. It used to be that only uneducated people made mistakes with these two words (and also with she/her, he/him, we/us, they/them). Everyone knew about parts of speech and sentence structure and correctly used **I, she, he, we** and **they** as subjects (the ones taking the action) and **me, her, him, us** and **them** as objects (the ones receiving the action). Nowadays one's ears are assailed daily by misusages from all directions: radio, TV, newspapers ... Just about everyone seems to have jumped aboard this ungrammatical bandwagon. The problem is most acute when the objective case is called for, as here:

*I gave it **to him**.*

*He wrote it **for** my sister **and me**.*

*She told all **of us** about it.*

The problem seems to be those little prepositions **to, for** and **of**. Whenever a preposition is involved, people get tangled up and produce whoppers such as these:

*It was designed **for we** mothers.*

*Jim said it **to her** and I.*

I heard these examples on TV. The second one is puzzling since it is inconsistent in mixing an objective **her** with a subjective **I**. But it is also particularly popular. Whenever there are two people mentioned, the one farthest away from the preposition is usually in an incorrect form.

Is it any wonder that I have about given up on grammar? □

THE MATTER OF STYLE

J2

P.L. 86-36

A CRYPTOLOG article on writing memos [1st Issue, 1987] prompted me to ask: which letters or memos that pass through the Executive Registry are truly memorable? Not many, and if they are, it's usually for the wrong reason.

Most writers don't think about style. It's hard to explain what style is, much less how to achieve it. What causes a combination of words to leap from the page, to be recalled later? Consider restating this sentence, "These are the times that try men's souls" as "Soulwise, these are trying times." Not quite the same.

Before you can think of style, you must know the principles of English composition. Learn to recognize and use properly the eight parts of speech. Diagram a few sentences for practice. Learn the rules of punctuation, improve your spelling by looking up doubtful words in a good dictionary, and concentrate on the fundamentals of a plain English style.

Brevity will help most to develop or improve style. "OMIT NEEDLESS WORDS" shouts Strunk. He says: "Vigorous writing is concise. A sentence should contain no unnecessary words, a paragraph no unnecessary sentences, for the same reason that a drawing should have no unnecessary lines and a machine no unnecessary parts. This requires not that the writer make all his sentences short, or that he avoid all detail and treat his subjects only in outline, but, that every word tell." What an essay on the nature and beauty of brevity!

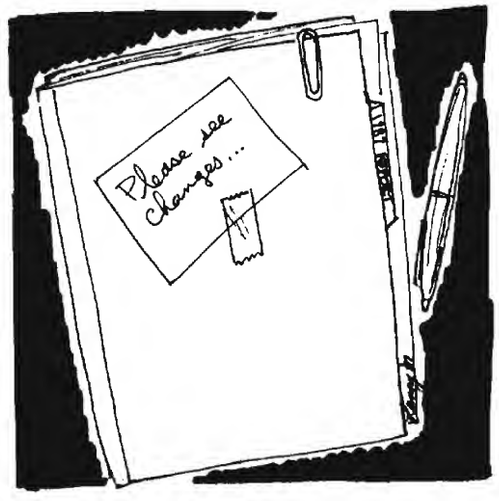
Strunk also advises writers to revise and rewrite. Few writers get it right the first time. Have someone else check your work; others can spot your errors much more quickly that you can. To hold your reader's attention, use definite, specific and concrete language. And be clear. There is no substitute for clarity. Ambiguity may amuse, but humor is not the aim--clarity is. □

Solution to NSA-Crostic # 65, 3rd Issue 1987

Ronald Reagan, DEDICATION
(Plaque on Ops 2B)

You of the N[ational] S[ecurity] A[gency] are . . . part of a proud tradition, . . . which . . . has its beginnings with George Washington and the American Revolution. And you . . . make history quietly – silently – aware that . . . your greatest victories, if ever known at all, will be divulged only . . . many years from now.

How to Measure Clarity in Writing



[redacted] *R451*

Inspiration for this article came from [redacted] and her article, "How to Write a Memo" [CRYPTOLOG, 1st Issue 1987]. Guideline 4 in her article addressed how to write simply and clearly, and it included some helpful rules. But the article did not explain how to measure the clarity of writing.

I found a simple way to measure the readability of a piece of writing. It's a guideline called the Gunning "Fog Index," first published by Robert Gunning in 1952.

The guidleine does have two minor drawbacks. First, its simplicity results in a measure that is not exact. And second, the index says nothing about the writer's style. However, the value of the guideline's simplicity far outweighs the disadvantages for making it a useful writing aid.

Here are the steps for making the calculation.

1. Using a writing sample that is at least 100 words long, find the average number of words per sentence. Divide the total number of words in the sample by the number of sentences. This gives you the average sentence length.

2. Count the number of words having three syllables or more in a 100 word passage. Don't count: (a) words that are capitalized; (b) combinations of short easy words like "bookkeeper;" or (c) verbs of three syllables whose third syllable is "ed" or "es," as in "created" or "trespasses."

3. Add the results of steps 1 and 2 and multiply by 0.4. This will be the Fog Index. It corresponds roughly with the number of years of schooling a person would require to read a passage with ease and understanding.

Fog Index	Readability
5	fairly easy
7-8	standard
9-11	somewhat difficult
12-15	difficult
17 +	very difficult

(Isn't it interesting that the "standard" level of writing corresponds to the comprehension level of an 8th grade education?)

Sentence length and word complexity are the major factors that determine readability. But don't go overboard while trying to achieve a lower Fog Index. Writing that contains all short sentences with one syllable words would read like a first grade primer.

Again, let me say that the result of the guideline is not precise. But a sample having a Fog Index of 10 certainly will be clearer than one with an index of 15.

Practice using the guideline on the first 8 sentences in this article. You should get a Fog Index of about 8.6.

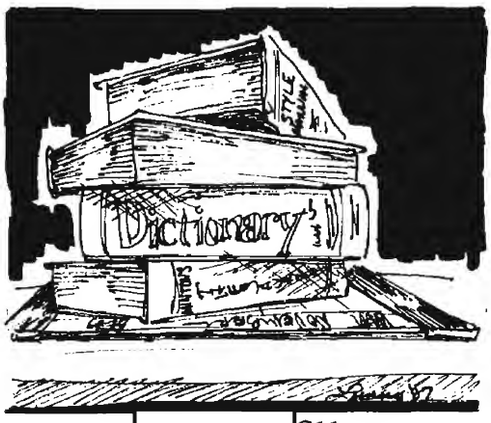
1. Average sentence length is 13.5.
2. Number of words equal to or greater than three syllables is 8.
3. Fog Index is $(13.5+8) \times 0.4 = 8.6$.

Don't skip over this part; go back and do it!

Now try the Gunning Fog Index on some of your own writing; you may be surprised at the results. Is your writing too complicated for others to understand? Perhaps you can improve it by breaking those long sentences into two separate thoughts? Substituting simple words for long ones should help, too.

How does your writing measure up? □

Two Tips on Writing



C11

¶

Two common abbreviations that are often misused are "i.e." and "e.g." They are especially nagging since you may not even find them in your desktop dictionary. Most people know that one of them (i.e., as it turns out) means "that is" and the other (e.g.) means "for example." The problem is remembering which is which. The result of guessing wrong is that you may say "that is" and give an example (or series of examples) instead of an explanation, or vice versa. If you don't mean for your list to be exhaustive, be sure to say "for example" (e.g.). On the other hand, if you mean to explain or amplify, use i.e.

How to tell the difference? The easy way is to remember the expansion of one of them: i.e. stands for the Latin expression *id est*, which means *it is* or "that is." Even if you didn't study Latin or a Romance language, this one should be easy to remember. Id and est look enough like "it" and "is" to give you a hint. By the way, Freud used the Latin *id* when he came up with his terminology. Of course, if you prefer, you can remember the expansion of e.g., which is *exemplia gratia*.

Examples:

> "The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system." [Files and programs are two examples among several possibilities for named objects.]
>
> "Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity." [Passwords are among several possible mechanisms.]
>
> "When the TCB exports an object to a mutilevel I/O device, the sensitivity label associated with the object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., "machine-readable" or "human-readable form)." ["Machine-readable" and "human-readable" explain what is meant by the same form; they are not examples of several kinds of same form.]

Note the form of the abbreviations: a period follows each letter, but there is no space between the first period and the second letter. A comma typically follows the abbreviation.

¶

Does a sentence-ending period precede or follow the parenthesis or quotation mark? This is the *bête noire* of many of us. When a period is used next to a parenthesis, the rule is completely logical: if the parenthetical expression is PART of a sentence, the period follows it. If the parenthetical expression CONTAINS the sentence, the period precedes the final parenthesis.

When a quotation occurs as the last element of a sentence, the rule differs. Even though the quotation is completely within the sentence, the period precedes the final quotation mark. The reason for this is that typographers feared that the little period would be lost if it fell completely outside the sentence. For the same reason, a comma is placed within the quotation marks. An exception is made for technical text, wherein a distinction must be made between "period—quotation mark" and "quotation mark—period."

Examples:

> The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on the any other subject (unless restrained by mandatory access control).
>
> (See the Convert Channel Guideline section.)
>
> Any discussion of computer security necessarily starts from a statement of requirements, i.e., what it really means to call a computer system "secure."
>
> The result of executing "substr (alph, 3,5)" is "abc". [If the period preceded the hyphen, the result would be interpreted as "abc.", which is incorrect.] □

Pointers on Grammar

[redacted] P12

The article on memos by [redacted] impelled me to pass on some pointers on grammar that readers might find helpful.

About hyphenation

My grammar teacher gave us a rule about hyphenation that works:

- If the sentence makes sense using each of the modifiers separately, don't hyphenate. Example: "We have a large red barn." It makes sense to say, "We have a red barn" and it also makes sense to say "We have a large barn." So we don't hyphenate.

- If the sentence doesn't make sense using each of the modifiers separately, hyphenate. Example: "He had a broken-down car." You might say "He had a broken car," but you wouldn't say, "He had a down car."

Misuse of quotes

My biggest pet peeve with regard to grammar is the misuse of quotes, especially partial quotes. The rule is, almost always, that commas and final periods go inside quotation marks. Other punctuation marks should be placed inside the quotation marks only if they are a part of the matter quoted. Here are some correct examples:

Call it a "gentlemen's agreement."

Why call it a "gentlemen's agreement"?

"Change 'cat' to read 'dog'."

One reason why many NSAers misuse partial quotes is that they subconsciously follow British usage, which is to put quotes inside the period or comma. That's understandable. What isn't understandable is the inconsistency; many memos have it both ways -- sometimes in, sometimes out.

The reason isn't *because*

"The reason is because" is incorrect because the verb is requires an adjective or noun clause following. The correct form is: *the reason is that . . . The reason why . . . is.*

It's not "kind of a"

People say, "I like that kind of a meal." when they should say, "I like that kind of meal." Use of the indefinite article a limits the field to one thing. In this case, there is only one thing to choose from meal, not a class of things.

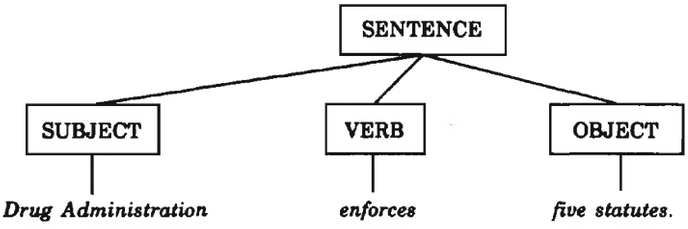
It's not "very unique"

When people say, "I had a very unique experience," they are probably confusing *unique* with *unusual.* Unique means one of a kind. It is an absolute that cannot be qualified.

Editor's Note:

Discussion on writing in these pages is now closed. We refer readers to the many works on grammar, usage, and style that can be found in libraries and bookstores. We will, however, consider articles on SIGINT terminology and usage.

THE HERO OF THE SENTENCE



Extract from: *Getting Your Ideas Across Through Writing,* Training Manual No. 7, 1950. US Department of Health, Education and Welfare.

The hero of the sentence is the "hero" of the story that each sentence tells. The "subject" is what the story's about. For some strange reason, we often pick the wrong hero, as in this sentence:

> The function of the Food and Drug Administration is the enforcement of statutes to insure the honesty and purity of foods, drugs, devices and cosmetics. (This is the opening sentence of a pamphlet.)

Who cares to read a story about a "function"! The Food and Drug Administration is the hero of this story, so let's make it the subject: *"The Food and Drug Administration"* (Let's make the verb work, too.) *"enforces five statutes . . . "*

Of course we cannot take time to fiddle that way with each sentence. Many of us need to change our habits, however, because we habitually go out of our way to select the wrong subject. People like to read about people and concrete things; yet often we twist the sentence around so that the story appears to be about an abstraction.

Most of all, people like to read about people. Yet readers of Government writing must get the impression that no human beings exist, anywhere. Our sentences tell stories about functions, policies, grants, conditions, factors, abstract ideas, and "it" – especially "it." Everything but people. *Ours are programs for people, administered by people,* yet often we write like this:

> *Employment* in manufacturing recorded increases, while there were declines in trade and domestic service. (The *number of people* working in manufacturing increased, while the number in trade and domestic service decreased.)

When we do admit that people exist, we often treat them as mere appendages to abstract ideas. Sometimes we seem to go out of our way to keep from making them the subject of our sentences, like this:

> The *protection* afforded industrial workers is far from complete. (Many *industrial workers* are inadequately protected.)
>
> *General Assistance or relief* accounted for nearly all the remaining recipients of public aid. (Nearly all the other *people* getting public aid were receiving general assistance or relief.)

Here are some more sentences in which the real "hero" has been subordinated. Just to focus your attention on the advantages of keeping people and relatively concrete things as the subjects, you may want to revise these sentences. You can make the verbs work more effectively, too.

> Responsibility for satisfactory working relationships within their organizational units rests with operating supervisors.
>
> Refusal of employment of women workers is common on the part of employers.
>
> There has been much opposition to the measure on the part of the educators. □

Gimme Rewrite!

Va.

This is a note to prospective contributors and to others who might have to write at NSA.

We hope that the articles on good writing in this issue do not discourage you from contributing because you're afraid of making one of the errors mentioned. As writing errors go, most of the ones touched on are minor lapses which are taken care of by the copy editor.

Self-respecting publishers of books, magazines, and newspapers all have copy editors as a matter of course. In many newspapers this tedious job is assigned to the reporter most recently hired . . . a lesson in humility.

The usual sequence of preparation for books and periodicals, including newspapers, is:

- § text editing;
- § copy editing;
- § proofreading.

Each should done by a different person. (In CRYPTOLOG, a low-budget rag, the Editor merely changes hats.)

The point that the authors of the articles are making is that the finished product should not contain such errors. They detract from and tend to cast doubt on the substance. Think of it as good grooming. However elegant and stylish your clothes may be, spots and tears are what people will notice, not the couturier styling or bespoke tailoring.

What to do?

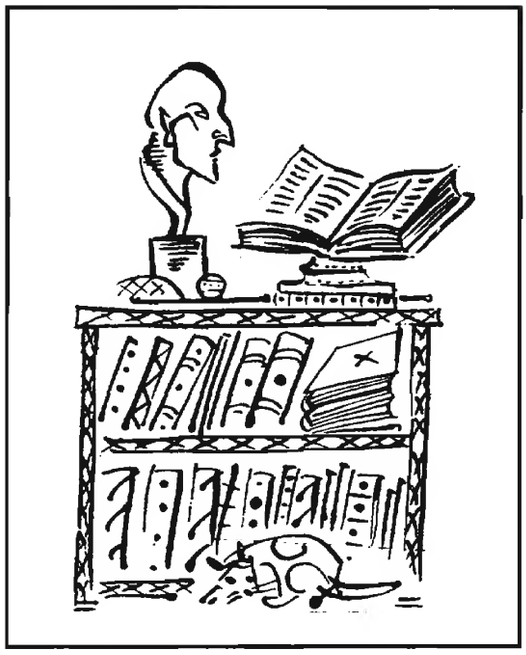
At a minimum, have someone else do your copy editing and your proofreading. (It is well known that you cannot do either for yourself because you tend to see what you expect to see.) But it's still better to hand over your bit of writing, along with sharp blue pencils, to at least one other person to edit for clarity. (And preferably, that person should come from the population of the intended reader.) This is what experienced writers do, and often, they expect their text to undergo changes in each of several passes by different individuals.

The wider the distribution of the document, the longer its life, the greater the care that you must give to preparation.

If you're doing any writing at all in this Agency, you should have at your desk some good references on grammar, usage, and editing. Order a desk copy for yourself. Browse in libraries and bookstores to determine which ones best suit your needs. Don't overlook handbooks for college students – some of them could have been written specifically for NSA!

Practice editing – a good way to begin. Try your hand at editing or rewriting an awkward passage, one that you had to reread to understand. Practice writing. A good exercise in writing clearly is writing up a suggestion.

Hardest of all, practice editing and rewriting your own text. Set it aside overnight, or a week, or a month, then read it cold. Now what do you see? □



Machine Translation: Past, Present, and Future. by W. J. Hutchins, University of East Anglia. Ellis Horwood Limited, Chichester, 1986 (distributed by Halsted Press, a division of John Wiley & Sons) [P 308 .H85]

Reviewed by: [redacted] *P12*

This book lives up to its comprehensive title. The "past" begins even before the 1948 memorandum by Weaver, from which all machine translation projects have sprung directly or indirectly, with a discussion of 17th-century numerical codes as universal languages, and a 1933 Soviet patent which went nowhere.

Weaver's memorandum justified the concept of machine translation in four ways, one of which will be of special interest to readers of CRYPTOLOG. During the war, a cryptanalyst had deciphered a Turkish message without knowing any Turkish. Weaver verified that this incident had actually happened. Hutchins explains that the relative frequencies of letters, digraphs, and so forth, are sufficiently similar in English and Turkish to have enabled the cryptanalyst to succeed. Weaver was mistaken, but in no way does that vitiate the concept of machine translation.

Hutchins points out that some prefer the term "computer translation" to machine translation, or MT, but declines to part with tradition.

He then surveys all, or so it seems, the MT systems for which information is available. His account of the Georgetown MT project was of particular interest to me, since it covers ground that I became aware of while a student there. His account is accurate, and it contains many details about the various approaches tried, and gives samples of the output produced. Included also are wryly humorous anecdotes about the rivalries that developed. His accounts of other MT approaches are similar.

Then came the infamous ALPAC (Automatic Language Processing Advisory Committee) report, which all but ended funding of MT projects in this country. Hutchins systematically demolishes the premises and methodologies of this report.

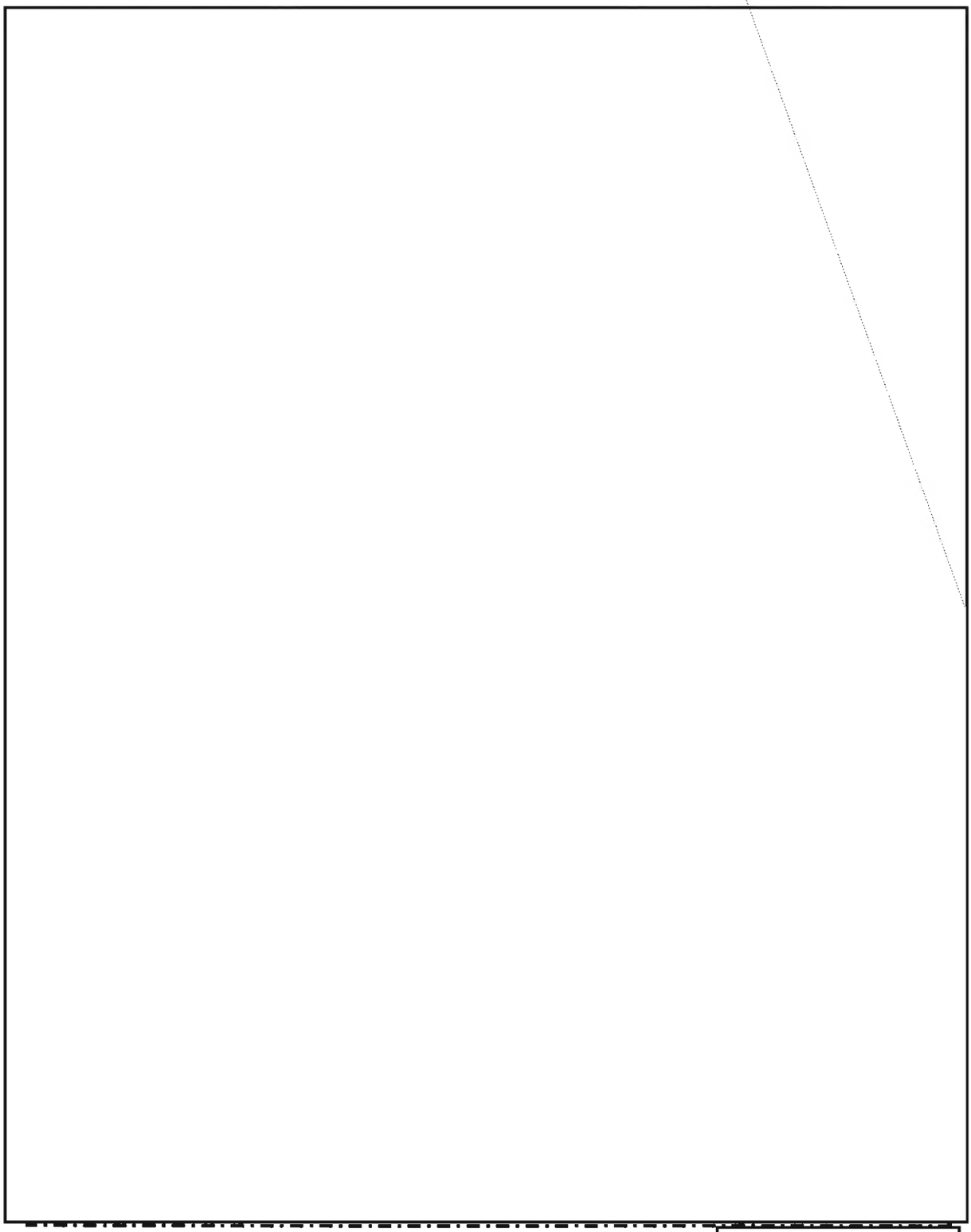
He then turns to the modern, or post-ALPAC, era of machine translation, describing a wide variety of projects and their applications in places such as Oak Ridge. Many statements in the ALPAC report and elsewhere ring hollow in the face of successes for MT in actual use.

A chapter on Artificial Intelligence approaches to MT concludes with the curious observation that its "feasibility in full-scale MT must, however, remain doubtful," eerily reminiscent of earlier dismissals of MT as a whole that the author himself has shown to be unfounded.

Although there are many translation applications for which MT is inappropriate, Hutchins's survey justifies his concluding remarks: "the future of MT is secure: it satisfies a genuine urgent need, it is the subject of worldwide research and development, and it is becoming a commercial product like other technical aids and office equipment; the application of the computer to translation is a reality, for many it is already as much a part of life as the computer itself." □

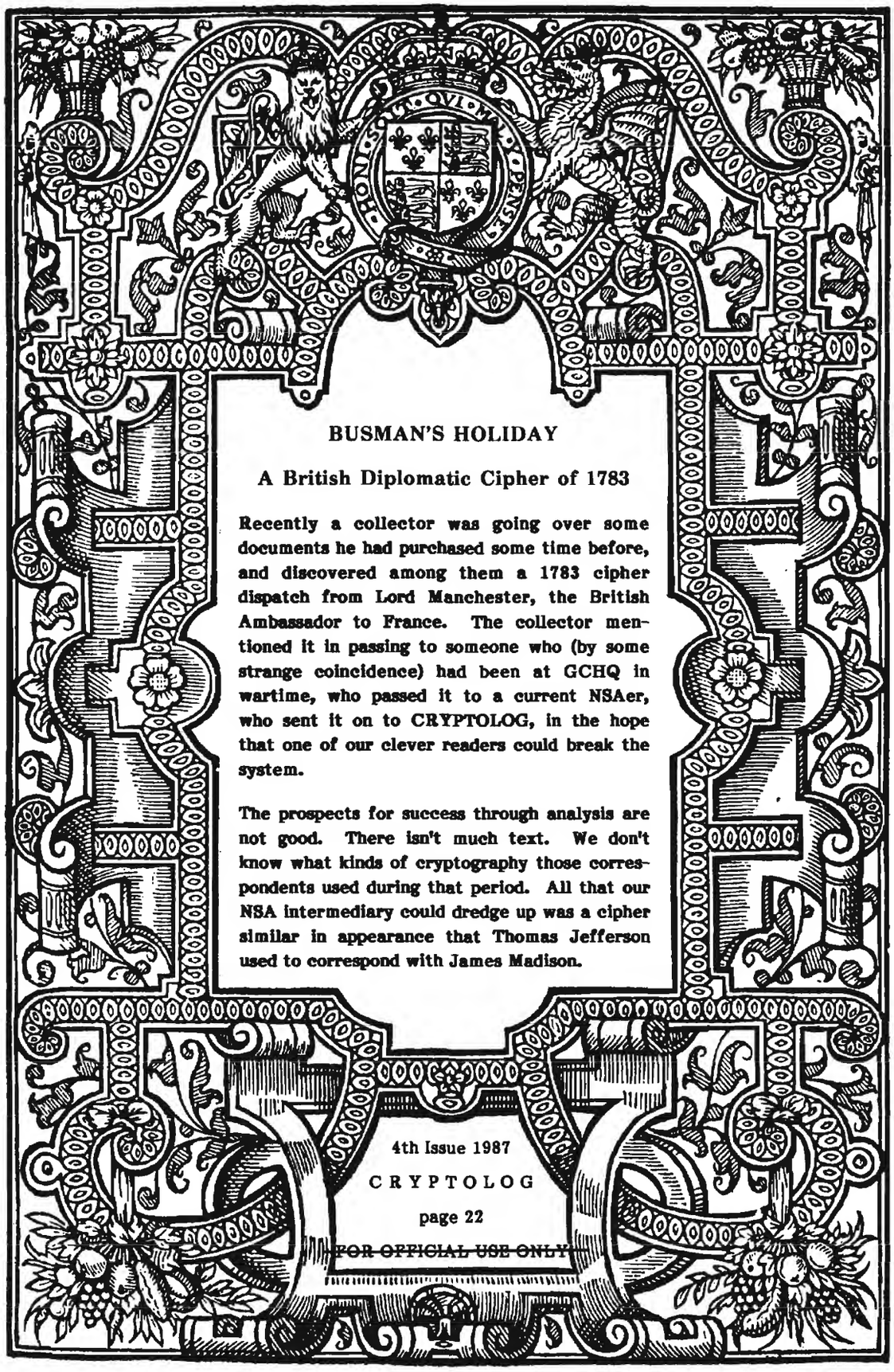
EO 1.4.(c)
P.L. 86-36

FROM THE PAST (U)



Provided by:

P.L. 86-36



BUSMAN'S HOLIDAY

A British Diplomatic Cipher of 1783

Recently a collector was going over some documents he had purchased some time before, and discovered among them a 1783 cipher dispatch from Lord Manchester, the British Ambassador to France. The collector mentioned it in passing to someone who (by some strange coincidence) had been at GCHQ in wartime, who passed it to a current NSAer, who sent it on to CRYPTOLOG, in the hope that one of our clever readers could break the system.

The prospects for success through analysis are not good. There isn't much text. We don't know what kinds of cryptography those correspondents used during that period. All that our NSA intermediary could dredge up was a cipher similar in appearance that Thomas Jefferson used to correspond with James Madison.

The Thomas Jefferson Cipher

The British Cipher of 1783

Fontainebleau Nov.r 20.1783

Sir,

I received your Letter dated Sept.r 2.d and should not have delayed so long sending an answer to it, had I any thing very material to communicate. 3693. 2517. 65. 3423. 576. 1100. 97. 1765. 3000. 259. 3032. 57. 66. 1795. 19. 211. 46. 1038. 1687. 970. 2609. 3369. 696. 3696. 427. 118. 3364. 1362. 456. 111. 566. 77. 1551. 2961. 1504. 1437. 3560. 1453. 2053. 1555. 1834. 1406. 9. 2044. 2694. 3423. 678. 1359. 493. 809. 1094. 956. 636. 1618. 61. 1437. 1369. 2316. 497. 314. 684. 1205. 193. 685. 2072. 65. 39. 3459. 3937. 2108. 2615. 1359. 766. 2450. 880. 1291. 647. 3339. 1175. 3714. 809. 184. 564. 2101. 1581. 566. 2323. 2066. 823. 665. 2401. 1692. 3560. 1444. 2734. 970. 330. 3601. 3263. 1612. 6000. 1291. 2000. 1936. 3056. 3278. 1618. 2894. 3438. 233. 2424. 3137. 3928. 1501. 3364. 434. 492. 566. 1498. 2450. 3560. 1603. 3905. 3082. 1504. 1242. 1624. 987. 2615. 1306. 350. 1245. 1504. 1145. 9. 3658.

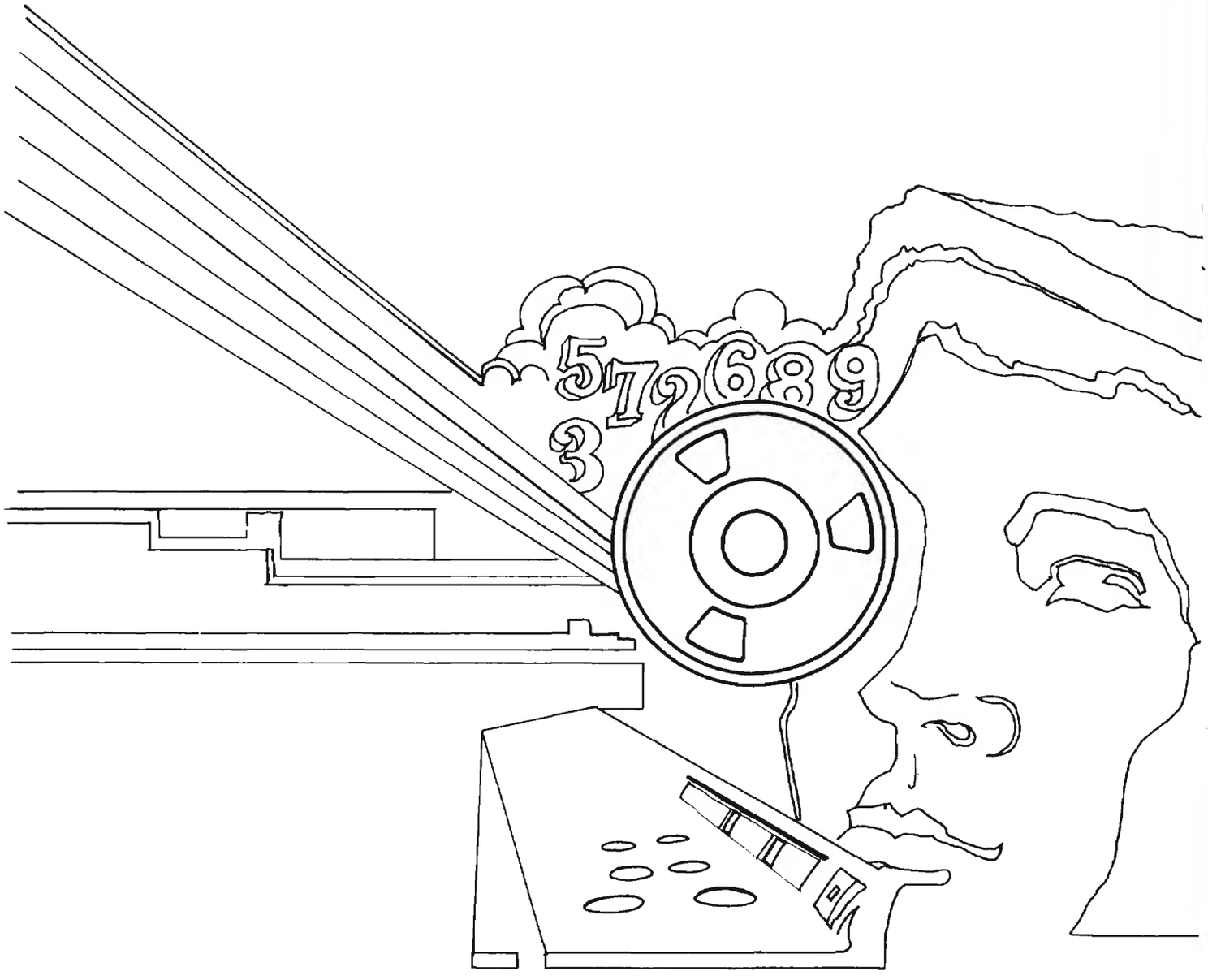
J.n John Thomson Secr.y

2622.

2622. 122. 3901. 1350. 758. 1986. 3905. 2426. 2051. 3791.
678. 498. 2109. 3438. 3536. 3487. 2999. 2694. 3892.
3056. 1350. 1397. 2485. 1778. 1719. 3739. 1753. 2126.
566. 77. . 956. 3000. 56. 9. 576. 3006. 10.

The Court is now at Fontainbleau where it is said it is to remain 'till late in November, notwithstanding the Pregnancy of the Queen.

I am
Sir,
With great regard.
Your Most Obedient
Humble Servant
Manchester


5726893